iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

CYBERSECURITY INVESTMENT UNDER RESOURCE CONSTRAINTS: OPTIMIZING SECURITY CONTROL SELECTION THROUGH RISK-BASED DECISION MODELS

Mojisola Ologe
Coauthor: Aisha Abdullahi

ABSTRACT
Digital infrastructure has become a critical asset for organizations as they continue to be targeted by persistent cybersecurity threats and are constantly battling for the limited financial, technical and human resources. Choosing security controls in this scenario goes beyond just prioritizing threats and buying the cheapest technology. It involves a systematic evaluation of the reduction in losses that can be expected from control investments, given organizational and operational requirements. This paper is an attempt to create a quantitative framework for the selection of cybersecurity controls in an optimized decision, taking into account the probability of threats, potential business impacts, control effectiveness, implementation cost, and resources available. The proposed framework is based on cybersecurity economics and quantitative risk assessment, and on combinatorial optimization, it defines control selection as a constrained optimization problem, with the objective of minimizing the residual expected risk. Security requirements are represented as explicit constraints, and staffing and implementation capacity are included with financial constraints. Additionally, the framework includes extensions for the risk estimates that are not certain and interactions between controls. The evaluation design involves comparing the proposed approach for optimization with cost-based ranking, risk-score prioritization, risk-reduction-per-cost heuristics, and greedy selection under the same resource limits. Sensitivity analysis and scenario testing are suggested to evaluate the robustness and applicability of the recommendations. The study introduces a clear modelling technique that will help in more defensible investments in cybersecurity, especially in enterprises that are not able to deploy all the security controls desired at once.

Keywords:
Cybersecurity investment, risk-based decision-making, security controls, constrained optimization, expected loss, control effectiveness, resource allocation, cyber risk management

I. INTRODUCTION

1.1 Background to the Study

Cybersecurity is an investment issue for organizations, not just a technical issue. Information systems are vital for providing services, performing financial transactions, handling sensitive information, and coordinating internal and external operations in organizations. These dependencies are vulnerable to threats that can cause business disruption, information compromising and significant recovery costs. Hence, proper cybersecurity should be achieved through the proper deployment of technical measures as well as rational decisions on the allocation of limited resources.

Economics is a well-known aspect of this challenge. Gordon and Loeb (2002) created an economic model for investments in information security that takes into account the vulnerability of information, and the possible loss in case of a breach. Their analysis questioned the notion that the most susceptible information assets always get the most investment. An organization can benefit more economically from investing in other areas where protection is not so costly. This important insight still holds true: the risk that poses the greatest possible reduction in risk per dollar is not always the risk that is most dangerous.

Anderson and Moore (2006) also showed that the economic incentives and organizational relationship have a greater effect on cybersecurity outcomes than just the technical design. Information asymmetry and externalities as well as the difference between the parties who pay for protection and those who suffer if it fails can affect security decisions. These factors make it difficult to allocate cybersecurity resources, especially if the organizations rely on shared cybersecurity systems or third-party service providers.

The difficulty in its application becomes greater when an organization is not able to put in place all the desired controls. For example, if your small business is considering upgrading its backup and recovery strategies, endpoint protection, identity management, or expanded security monitoring. The options each tackle a different risk aspect. A low-cost control might help to mitigate some of the threats; a high-cost specialist control might help to mitigate

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

a more limited set of threats. This determination can't be made with a degree of certainty based on price or technical sophistication.

The economic analysis, game theory and combinatorial optimization approaches have been proposed to tackle this issue in cybersecurity investment models. Böhme and Kataria (2006) reviewed models that could be employed for modelling information security risk and cyber insurance, and later research evolved decision support techniques based on financial pressures for allocating security controls. For instance, Radanliev et al. (2018) proposed constrained optimization models for allocating security controls and took into account uncertainty in vulnerability assessment. Later, Sawik (2022) showed the applicability of mixed-integer linear programming to investments in cybersecurity within the Industry 4.0 supply chain.

Risk management frameworks offer an important complementary base. National Institute of Standards and Technology (NIST) says the key factors in determining organizational risk are assessing threat sources, vulnerabilities, likelihood, and consequences (National Institute of Standards and Technology [NIST] 2012). The Cybersecurity Framework (CSF) Version 1.1 also offers a systematic way to identify, prioritize, and manage cybersecurity outcomes with respect to the organization's goals and resources (NIST, 2018). Such frameworks serve to direct risk-informed decision making, but the organization still needs to decide what combination of controls is feasible to address the organization's specific exposure.

The main obstacle is not just to find out what controls are useful. It's about finding the optimal mix of controls to maximize the reduction of organizational risk with the resources at your disposal. This demands an integrated approach which links risk exposure, control performance, implementation cost, and operational feasibility in a single decision-making framework.

1.2 Statement of the Research Problem

Cybersecurity control selection is frequently complicated by incomplete information, competing organizational priorities, and limited implementation capacity. Conventional approaches may rank controls by severity of associated threats, qualitative risk scores, compliance requirements, or cost-effectiveness ratios. These methods can support initial screening, but they do not necessarily identify the best combination of controls when resources are constrained.

A principal limitation of independent ranking is that the value of a control depends on the wider portfolio in which it is implemented. Two controls may address substantially overlapping risks, making their combined benefit smaller than the sum of their individual estimated benefits. Conversely, a preventive control and a recovery control may provide complementary protection by reducing both the likelihood and consequences of an incident. Control dependencies, implementation requirements, and differences in effectiveness can therefore alter the preferred investment portfolio.

The problem is further complicated by uncertainty. Threat probabilities are estimates, incident impacts vary, and the effectiveness of a control in practice may differ from its nominal or vendor-reported performance. Sánchez-García et al. (2023) identified continuing challenges in cybersecurity risk assessment, including incomplete coverage of assessment activities and difficulties in identifying the variables needed for accurate risk estimation. A control-selection model that treats every input as precisely known may consequently produce recommendations that are less reliable than their numerical precision suggests.

Existing research provides valuable foundations, but a decision-support model must translate risk estimates into feasible investment choices while accounting for the constraints relevant to a particular organization. It must also distinguish discretionary investments from mandatory security requirements. An optimizer that excludes a required control because another investment produces a larger estimated reduction in financial loss may generate an economically attractive but unacceptable recommendation.

This study addresses the problem by developing a risk-based optimization framework that selects cybersecurity controls according to their contribution to reducing expected residual risk, subject to budgetary, operational, and mandatory-control constraints. Its proposed evaluation compares optimization with established prioritization heuristics under consistent assumptions, allowing the value of portfolio-based decision-making to be assessed rather than presumed.

1.3 Aim and Objectives of the Study

The aim of this study is to develop and evaluate a quantitative decision-support model for optimizing cybersecurity control selection under resource constraints.

The specific objectives are to:

1) Examine existing cybersecurity investment, risk assessment, and control-selection models.
2) Formulate a constrained optimization model integrating threat probability, potential impact, control effectiveness, implementation cost, and resource availability.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

3) Incorporate mandatory security requirements and represent important interactions between controls where sufficient information is available.
4) Compare the proposed model with conventional control-prioritization methods under equivalent resource constraints.
5) Evaluate model sensitivity, robustness, and computational feasibility across different scenarios.
6) Derive practical recommendations for organizations seeking to improve cybersecurity investment decisions with limited resources.

1.4 Research Questions

The study is guided by four research questions:

RQ1: How can threat probability, potential business impact, control effectiveness, and implementation cost be integrated into a constrained cybersecurity control-selection model?

RQ2: How does the proposed optimization model compare with conventional risk-ranking and cost-effectiveness methods under equivalent resource constraints?

RQ3: How do uncertainty, control dependencies, and multiple operational constraints affect the selection of cybersecurity controls?

RQ4: How stable and practically useful are the model's recommendations across different budget levels and organizational scenarios?

1.5 Research Contribution and Significance

The principal contribution is a structured optimization framework that connects quantitative cyber-risk assessment to practical security control selection. Rather than evaluating each control independently, the model evaluates portfolios of controls against a common residual-risk objective and explicit resource constraints. The methodological contribution lies in making the decision variables, risk parameters, control-effectiveness assumptions, and constraints transparent. This facilitates reproducibility and allows decision-makers to examine why particular controls are selected or excluded.

The practical contribution is a framework for comparing feasible investment alternatives. It is intended to help cybersecurity managers justify expenditure, identify resource bottlenecks, assess the consequences of budget changes, and communicate residual-risk trade-offs to organizational leadership. The study does not assume that optimization will outperform every heuristic in every situation. Instead, it proposes a controlled evaluation to determine when portfolio-based optimization offers meaningful advantages, when simpler approaches may be adequate, and how uncertainty affects the resulting recommendations.

1.6 Scope and Delimitations

The study focuses on organizational cybersecurity investment and the selection of preventive, detective, responsive, and recovery controls. The primary analytical objective is the minimization of expected residual financial loss over a defined planning horizon, subject to mandatory security requirements and resource constraints.

Financial resources, personnel availability, implementation time, and technical capacity are considered relevant constraints. Non-financial consequences, including regulatory exposure, service disruption, and reputational harm, are recognized as important but are not assumed to be fully monetizable. Where appropriate, these consequences are represented through additional constraints or separately reported risk indicators.

The core formulation is a static portfolio-selection model. Dynamic investment decisions, strategic attacker behaviour, and extensive network-wide interdependencies are outside the initial model unless explicitly introduced as extensions. These delimitations keep the central problem mathematically manageable while identifying directions for further development.

II. LITERATURE REVIEW AND THEORETICAL FOUNDATION

2.1 Cybersecurity Investment and Resource Allocation

Cybersecurity investment can be understood as the allocation of resources to reduce the probability or consequences of security incidents. Unlike investments whose returns can be observed directly through increased production or sales, security investments often generate value through losses avoided. This makes their economic justification difficult, particularly when incident data are sparse and counterfactual outcomes cannot be observed directly.

Gordon and Loeb (2002) established a foundational economic perspective by linking investment decisions to information vulnerability and expected breach losses. Their model showed that the relationship between vulnerability and optimal expenditure is not necessarily linear. Bojanc and Jerman-Blažič (2008) extended the economic perspective by presenting an approach to information-security risk management that connects asset valuation, threats, vulnerabilities, and security investment.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

These approaches demonstrate the value of considering economic consequences alongside technical risk. However, determining an overall investment level differs from selecting a portfolio of discrete controls with different costs, coverage, and resource requirements. A portfolio model must consider the combined contribution of controls and whether their implementation is feasible within the organization's constraints.

Fedele and Roner (2022), in their review of cybersecurity investment research, distinguished between models involving individual firms and those involving interdependent organizations. Their synthesis illustrates the diversity of economic approaches and the importance of organizational context. For the present study, the individual organization provides the primary decision-making unit, while the implications of shared infrastructure and interdependence are considered when discussing model limitations.

The resource-allocation problem is therefore characterized by three connected decisions: which risks deserve priority, which controls can reduce those risks, and how the available resources should be distributed across the feasible alternatives. The proposed model focuses on the third decision without treating the first two as independent of it.

2.2 Cybersecurity Risk Assessment and Quantification

Risk assessment provides the inputs required for rational control selection. In a simplified quantitative formulation, expected loss is expressed as the probability of an adverse event multiplied by its associated loss. For multiple threat scenarios, the individual expected losses can be aggregated when the underlying assumptions justify doing so.

NIST SP 800-30 Rev. 1 describes risk assessment as a structured process involving threat sources, threat events, vulnerabilities, likelihood, and consequences (NIST, 2012). This framework supports a systematic understanding of risk but does not require every organization to use a single numerical risk model.

Quantitative approaches can offer greater analytical transparency than qualitative labels alone. Nevertheless, numerical estimates are only as reliable as their underlying data and assumptions. A probability estimate derived from historical incident frequency may not accurately represent a changing threat environment, and a financial impact estimate may omit important indirect consequences.

Sánchez-García et al. (2023) reviewed cybersecurity risk assessment tools and identified variations in the models, variables, and stages covered by existing approaches. Their work reinforces the need to specify precisely how risk inputs are obtained and used. Cheimonidis and Rantos (2023), in their systematic review of dynamic cybersecurity risk assessment, also highlighted the limitations of static approaches in environments where threats and vulnerabilities evolve rapidly.

Quantitative risk assessment is particularly relevant to the present study because the proposed optimization model requires comparable estimates of baseline risk and residual risk. However, the model should not confuse an estimated expected loss with a complete representation of organizational risk. Rare events with catastrophic consequences, non-financial impacts, and uncertain dependencies may require additional constraints or scenario analysis.

2.3 Security Controls and Their Effectiveness

Security controls differ in their purpose, implementation requirements, and effects on risk. Preventive controls seek to reduce the likelihood of successful attacks; detective controls aim to identify suspicious activity; and response and recovery controls seek to limit the consequences of incidents and restore operations.

The economic value of a control depends on the threat scenarios it addresses and the extent to which it changes their expected consequences. A backup solution may have limited influence on the probability of an intrusion but substantially reduce recovery costs. An access-control improvement may reduce the likelihood of unauthorized access across multiple assets. Treating both controls as if they produce the same kind of risk reduction would obscure their distinct functions.

Control effectiveness is also conditional on implementation quality. A technically capable monitoring system may offer little practical benefit if alerts are not investigated, while a backup strategy may fail if restoration procedures are not tested. The model therefore distinguishes nominal effectiveness from the effectiveness that an organization can reasonably expect to realize under its operational conditions.

A further challenge is overlapping coverage. If two controls protect against the same threat, their combined risk reduction cannot automatically be calculated by adding their individual effectiveness estimates. The portfolio model must either represent the interaction explicitly or state the simplifying assumptions under which the effects are combined.

2.4 Existing Cybersecurity Investment and Optimization Models

Research has developed several approaches to cybersecurity investment decisions. These approaches differ in their treatment of uncertainty, strategic behaviour, control interactions, and implementation costs.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Cavusoglu et al. (2004) examined information-security investment decisions and the economic implications of security breach information. Gordon and Loeb (2002) provided a foundational model for assessing the economically appropriate level of investment. These contributions establish why expenditure should be related to expected loss reduction rather than determined solely by technical exposure.

Bodin et al. (2008) investigated information-security investment decisions using the Analytic Hierarchy Process, illustrating how multiple criteria can inform the prioritization of security investments. Multi-criteria methods can incorporate organizational preferences and qualitative considerations, although their rankings depend on the criteria and weights selected. They do not necessarily solve the same portfolio-selection problem as a constrained optimizer.

A more direct approach is combinatorial optimization. Böhme and Kataria (2006) examined models and measures relevant to information-security risk and insurance, while Radanliev et al. (2018) developed constrained optimization models for allocating security controls under uncertainty in vulnerability assessment. Their work is particularly relevant because it treats security configuration as a decision problem involving alternative control choices rather than only a ranking exercise.

Bodin et al.'s multi-criteria approach and the optimization approach are complementary, but they serve different purposes. A ranking method can help determine the relative importance of factors, whereas a portfolio optimizer determines which combination of controls best satisfies a defined objective and resource limits. This distinction matters when controls compete for the same limited budget or when several controls provide overlapping protection.

Stochastic optimization offers another extension. Paul and Zhang (2021) proposed a two-stage stochastic programming model for cybersecurity risk planning involving firms, government, and an attacker. Their work incorporates resource allocation and the consequences of detection and containment delays. Sawik (2022) formulated a mixed-integer linear programming model for cybersecurity investment in Industry 4.0 supply chains, illustrating how a complex investment problem can be represented through mathematical programming.

Together, these studies demonstrate that optimization is an established approach to cybersecurity investment. Consequently, the contribution of the present study cannot rest on the use of optimization alone. It must be grounded in the precise combination of risk parameters, resource constraints, portfolio assumptions, and evaluation procedures adopted by the proposed framework.

2.5 Synthesis of the Literature and Research Gap

The literature establishes three relevant findings. First, cybersecurity investment should be evaluated in relation to expected loss and the economic consequences of incidents (Gordon & Loeb, 2002; Bojanc & Jerman-Blažič, 2008). Second, control selection is a portfolio problem in which costs, risk coverage, and resource constraints influence the feasibility and value of different combinations (Radanliev et al., 2018; Sawik, 2022). Third, risk assessment and investment decisions are affected by uncertainty, incomplete information, and the changing threat environment (Sánchez-García et al., 2023; Cheimonidis & Rantos, 2023). These findings also establish a caution: the proposed model should not claim that prior research has ignored constrained optimization or uncertain control selection. Such approaches already exist. Instead, the study focuses on developing a transparent formulation that integrates expected residual loss, control effectiveness, lifecycle cost, budget limits, and operational constraints, then evaluates its recommendations against clearly defined baseline methods.

The research gap is therefore operational and evaluative. The study seeks to provide a reproducible framework in which the assumptions governing control effectiveness and portfolio interactions are explicit, mandatory controls are distinguished from discretionary choices, and the performance of the resulting portfolio can be compared under equivalent constraints.

The intended contribution is a decision-support model and evaluation protocol. Its effectiveness must be demonstrated through computational or empirical analysis rather than inferred from the mathematical formulation alone.

2.6 Theoretical and Conceptual Foundation

The study draws primarily on decision theory, cybersecurity economics, risk management, and constrained optimization.

Decision theory provides the basis for comparing alternative actions under uncertain outcomes. Cybersecurity economics explains why investments should be evaluated in relation to expected losses and the costs of protection. Risk management establishes the need to identify, assess, treat, and monitor risks in accordance with organizational objectives. Constrained optimization provides the mathematical means of selecting a feasible portfolio from competing control alternatives.

Conceptually, the model links five main elements:

1. **Threat exposure:** the probability or frequency of threat scenarios and their potential consequences.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

2. **Control effectiveness:** the extent to which each control reduces the likelihood or impact of relevant scenarios.
3. **Investment cost:** the financial and operational resources needed to implement and maintain each control.
4. **Feasibility constraints:** the budget, staffing, time, technical capacity, and mandatory requirements governing selection.
5. **Residual risk:** the expected exposure remaining after the selected controls are implemented.

The model's primary outcome is the expected residual risk associated with the chosen portfolio. Secondary outcomes include total investment cost, resource utilization, and the stability of recommendations under changing assumptions.

III. RESEARCH METHODOLOGY

3.1 Research Design

The study adopts a quantitative model-development and computational-evaluation design. The research proceeds through four stages: mathematical formulation, implementation of the optimization procedure, comparison with baseline methods, and sensitivity and robustness analysis.

The initial evaluation can use synthetic benchmark data to ensure that the model's behaviour can be examined under controlled conditions. Where reliable organizational data are available, an additional case study can be used to assess practical applicability. Synthetic data will be identified as illustrative rather than treated as empirical evidence of real-world cybersecurity performance.

3.2 Model Scope and Assumptions

The core model assumes that an organization faces a finite set of relevant threat scenarios and has a defined set of candidate security controls. Each control has an estimated implementation cost, a resource requirement, and an effectiveness profile across the threat scenarios.

The organization operates under a fixed planning horizon and a specified set of resource limits. Mandatory controls are treated as requirements rather than discretionary alternatives. The initial formulation assumes that the probability and impact estimates are fixed inputs, with uncertainty addressed in subsequent scenario and sensitivity analyses.

For the baseline model, control effects are assumed to combine multiplicatively where multiple selected controls mitigate the same threat. This is a simplifying assumption, not a universal property of security controls. Extensions will be needed when control interactions, conditional dependencies, or correlated threat scenarios materially affect risk.

3.3 Model Notation and Parameters

Let:

- $i = 1, ..., n$: Index of threat scenarios.
- $k = 1, ..., K$: Index of candidate security controls.
- p_i: Probability of threat scenario i occurring within the planning horizon.
- L_i: Potential financial loss associated with scenario i.
- e_{ik}: Estimated effectiveness of control k against scenario i, where $0 \leq e_{ik} \leq 1$.
- C_k: Lifecycle cost of implementing control k over the chosen planning horizon.
- B: Available cybersecurity budget.
- a_{rk}: Quantity of resource r required by control k.
- b_r: Available quantity of resource r.
- $x_k \in 1$: Binary decision variable indicating whether control k is selected, where $x_k = 1$ if selected and $x_k = 0$ otherwise.

The resource index (r) can represent personnel hours, implementation capacity, or another measurable resource. The units must be defined consistently for each constraint.

3.4 Baseline Risk Estimation

For a simplified set of mutually exclusive or otherwise appropriately aggregated threat scenarios, baseline expected loss is expressed as:

$$R_0 = \sum_{i=1}^{n} p_i L_i$$

This quantity represents expected loss over the defined planning horizon. It is not necessarily the maximum possible loss, the worst-case outcome, or a complete measure of organizational risk.

Where the scenarios overlap, are dependent, or can occur repeatedly, the aggregation must be adjusted to avoid double-counting and to distinguish event probability from event frequency. The baseline model therefore requires an explicit threat-scenario definition before the equation is applied.

3.5 Residual-Risk Formulation

For the initial model, the residual loss associated with threat scenario (i) is represented as:

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

$$L_i \prod_{k=1}^{K} (1 - e_{ik}x_k)$$

Expected residual risk is then:

$$R(x) = \sum_{i=1}^{n} p_i L_i \prod_{k=1}^{K} (1 - e_{ik}x_k)$$

This formulation assumes that the selected controls independently reduce the residual risk associated with each scenario under the specified effectiveness estimates. It provides a tractable starting point for modelling overlapping protection, but it may not adequately represent common-mode failures, prerequisites, or controls whose effectiveness depends on other controls.

An alternative formulation will be required if controls act on different stages of an attack, affect incident probability and severity in different ways, or exhibit significant dependencies. The model should not apply the multiplicative expression without evaluating whether its assumptions are reasonable for the intended application.

3.6 Objective Function and Resource Constraints

The primary objective is to minimize expected residual loss:

$$\min_x R(x) = \sum_{i=1}^{n} p_i L_i \prod_{k=1}^{K} (1 - e_{ik}x_k)$$

subject to the budget constraint:

$$\sum_{k=1}^{K} C_k x_k \leq B$$

and resource constraints:

$$\sum_{k=1}^{K} a_{rk}x_k \leq b_r, \text{ for all } r$$

Mandatory security requirements are represented by fixing the relevant decision variables to one:

$$x_k = 1, \text{ for all } k \in M$$

where (M) is the set of mandatory controls. Additional constraints can impose minimum security baselines or maximum tolerable residual risk for critical threat scenarios.

This formulation separates the objective of minimizing risk from the constraints governing affordability and feasibility. If the study instead uses an objective that combines financial loss and investment expenditure, it must justify the economic interpretation of the combined terms and avoid double-counting costs already enforced through the budget constraint.

3.7 Optimization Method

The baseline model is a binary portfolio-selection problem. Because the residual-risk expression contains products of decision-dependent terms, it is not automatically a linear model. A suitable nonlinear or mixed-integer formulation, exact solver, or valid linearization method must be selected according to the problem size and the assumptions adopted.

For small instances, exact enumeration or an exact optimization solver can be used to establish a benchmark solution. For larger instances, heuristic methods may be evaluated against the best available solution or a valid optimality bound. Solver selection and linearization details should be documented to support reproducibility.

3.8 Evaluation Design

The model will be compared with four baseline approaches: cost-based ranking, risk-score ranking, risk-reduction-per-cost ranking, and greedy control selection. Each approach will use the same candidate controls, threat estimates, costs, mandatory requirements, and resource limits.

Evaluation metrics will include:

- Expected residual loss.
- Absolute and relative risk reduction compared with baseline risk.
- Total lifecycle cost and budget utilization.
- Compliance with mandatory and operational constraints.
- Portfolio stability under changing input assumptions.
- Computational runtime and solution quality.

The comparison will test whether optimization produces better portfolio-level outcomes under equivalent constraints. It will also identify conditions under which simpler prioritization methods produce similar results.

3.9 Sensitivity and Uncertainty Analysis

Sensitivity analysis will examine how changes in threat probability, impact, control effectiveness, and implementation cost affect the selected portfolio. Budget and staffing availability will also be varied to assess the marginal value of additional resources.

Where defensible probability distributions or uncertainty ranges can be specified, scenario-based or Monte Carlo analysis can examine the distribution of residual-risk outcomes. Robust optimization may be considered where the objective is to limit risk under a defined range of adverse parameter values.

These analyses will assess the stability of recommendations rather than assume that a single optimal solution remains best under all possible conditions.

3.10 Validation, Reliability, and Limitations

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Validation will involve checking the mathematical formulation, testing small instances against independently established solutions, verifying the computational implementation, and comparing performance with the selected baseline methods. Practical validation using organizational data or expert review may be conducted where appropriate evidence is available.

The model's limitations include uncertainty in threat and effectiveness estimates, possible dependence between threat scenarios, difficulty monetizing non-financial consequences, and the simplifying assumptions used to combine control effects. These limitations will be reported explicitly and considered when interpreting the results.

IV. MODEL APPLICATION AND ILLUSTRATIVE ANALYSIS

4.1. Illustrative Organizational Scenario

To demonstrate how the proposed model supports cybersecurity investment decisions, this section considers a hypothetical organization with a limited cybersecurity budget. The example is intended to explain the model's operation and does not represent an empirical case study or actual organizational data.

Assume that the organization faces three major threat scenarios: phishing-related compromise, ransomware, and unauthorized data exfiltration. Following an initial risk assessment, the estimated annual expected losses associated with these threats are assigned illustrative values of 40,000, 50,000, and 30,000 monetary units, respectively. The baseline expected annual loss is therefore 120,000 monetary units.

Management is considering three security controls: multi-factor authentication (MFA), enhanced backup and recovery, and endpoint detection and response (EDR). The controls differ in cost and effectiveness across threat scenarios. The organization has a maximum implementation budget of 50,000 monetary units.

The effectiveness estimates used in this example are hypothetical planning assumptions. In a real implementation, they would need to be supported by security testing, vendor evidence, historical incident data, expert assessment, or other appropriate sources.

Table 1. Illustrative threat scenarios and baseline expected losses

Threat scenario	Estimated annual probability	Loss if the event occurs	Expected annual loss
Phishing-related compromise	0.40	100,000	40,000
Ransomware	0.25	200,000	50,000
Unauthorized data exfiltration	0.15	200,000	30,000
Total	—	—	**120,000**

Note. Expected annual loss is calculated as the probability of a threat scenario multiplied by its estimated loss, assuming the probability and impact estimates represent the same assessment period.

4.2. Control Costs and Effectiveness

The model evaluates each control according to its implementation cost and estimated effectiveness against each threat scenario.

Table 2. Illustrative control portfolio parameters

Security control	Implementation cost	Phishing effectiveness	Ransomware effectiveness	Data-exfiltration effectiveness
Multi-factor authentication (MFA)	20,000	0.60	0.20	0.40
Enhanced backup and recovery	25,000	0.00	0.70	0.10
Endpoint detection and response (EDR)	30,000	0.30	0.50	0.50

Note: Effectiveness values represent assumed proportional reductions in the relevant scenario's expected loss for this illustration. They are not measured estimates of real-world performance.

The values indicate that MFA is particularly effective against phishing-related account compromise, while backup and recovery primarily reduce ransomware-related losses. EDR provides broader protection across the three scenarios. This variation illustrates why organizations should assess the relationship between individual controls and specific threats rather than assume that every control provides equal protection against every attack.

The estimates also highlight an important distinction: a control's effectiveness is threat-dependent. A control that performs well against one scenario may offer limited protection against another. Accordingly, a decision-support model should represent the effectiveness of each control against each relevant threat rather than assign one universal effectiveness score to an entire organization.

4.3. Comparing Alternative Control Portfolios

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Using the multiplicative residual-loss formulation introduced in Section 3, the residual expected loss associated with each threat is calculated by multiplying its baseline expected loss by the proportion of risk remaining after the selected controls are applied.

For the illustrative scenario, the residual loss for threat (i) is:

$$R_i(x) = p_i L_i \prod_{k=1}^{K} (1 - e_{ik} x_k)$$

The total residual expected loss is obtained by summing the residual losses across all threat scenarios.

Consider four alternatives: implementing MFA alone, backup and recovery alone, EDR alone, and combinations of two controls where the budget permits.

Table 3. Illustrative comparison of control portfolios

Selected portfolio	Total cost	Residual expected loss	Reduction in expected loss
No additional controls	0	120,000	0
MFA only	20,000	74,000	46,000
Backup and recovery only	25,000	82,000	38,000
EDR only	30,000	68,000	52,000
MFA + backup and recovery	45,000	44,200	75,800
MFA + EDR	50,000	40,200	79,800

Note: All figures are hypothetical. Residual expected loss is calculated using the stated effectiveness assumptions and the multiplicative model. The table does not include operating expenses, indirect implementation costs, or additional control dependencies.

Under the stated assumptions, the combination of MFA and EDR produces the lowest residual expected loss among the portfolios shown that satisfy the budget constraint. Its estimated residual loss is 40,200 monetary units, compared with 120,000 monetary units before the additional controls are introduced. The estimated reduction is therefore 79,800 monetary units, or 66.5% of the baseline expected loss.

The comparison demonstrates why selecting controls solely on the basis of individual effectiveness or cost can produce suboptimal outcomes. Although MFA is less expensive than EDR, its value is strengthened when combined with a complementary control. Similarly, the backup and recovery control performs well against ransomware, but the MFA–EDR combination produces a larger overall reduction across the particular threat scenarios and assumptions used in this example.

The results should not be interpreted as a universal recommendation to prioritize MFA and EDR over backup and recovery. A different threat profile, control cost, effectiveness estimate, regulatory requirement, or business dependency could change the optimal portfolio. In particular, backup and recovery may be mandatory for an organization whose operations cannot tolerate prolonged disruption. Where such requirements exist, the model should impose them as constraints before comparing the remaining investment options.

4.4. Interpretation of the Optimization Results

The illustrative analysis demonstrates four central features of the proposed decision-support model.

First, **the optimal portfolio depends on the organization's threat profile**. A control's value is determined not only by its technical capability but also by the likelihood and potential impact of the threats it addresses. A relatively inexpensive control may be a poor investment if it targets low-priority threats while leaving high-impact exposures largely unmitigated.

Second, **complementarity can influence portfolio performance**. Combining controls that address different stages or dimensions of an attack can reduce residual risk more effectively than concentrating resources on a single safeguard. Nevertheless, the multiplicative formulation assumes that the controls' residual-risk effects combine in a particular way. Real control interactions may be weaker, stronger, or dependent on implementation quality. These assumptions must therefore be tested rather than accepted automatically.

Third, **budget utilization should be evaluated against risk reduction, not spending alone**. The model does not recommend exhausting the available budget simply because funds are available. An additional control should be selected when its expected contribution to risk reduction, compliance, resilience, or another explicitly defined objective justifies its cost.

Fourth, **the model makes trade-offs visible**. Managers can compare feasible portfolios, examine the expected losses that remain after investment, and identify which risks cannot be adequately addressed within the available resources. This supports more transparent discussions about residual risk and the need for additional funding.

These observations are consistent with the wider cybersecurity investment literature, which has used optimization, stochastic programming, and economic models to examine security-control selection under resource constraints (Zhang et al., 2018; Schmidt et al., 2021; Tsiodra et al., 2023). Research on small-business cybersecurity investment, for example, illustrates how budget-constrained optimization can compare mitigation strategies while

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

accounting for uncertainty and the nonlinear relationship between investment and risk reduction (Tsiodra et al., 2023).

4.5. Incorporating Uncertainty into Control Selection

The deterministic illustration assumes that threat probabilities, loss estimates, effectiveness values, and control costs are known. In practice, these parameters are uncertain. Organizations may have limited incident histories, incomplete visibility into their systems, or insufficient evidence to estimate how effectively a proposed control will perform under real attack conditions.

A practical extension is to define a set of plausible scenarios, (s \in S), with scenario-specific probabilities, impacts, and control effectiveness values. The expected residual risk then becomes:

$$\min_x \sum_{s \in S} w_s \sum_{i=1}^{n} p_{is} L_{is} \prod_{k=1}^{K} (1 - e_{iks} x_k)$$

where (w_s) represents the weight assigned to scenario (s), with the weights summing to one when they represent probabilities.

This formulation allows management to assess whether a selected portfolio remains attractive under different assumptions about the threat environment. For example, an organization could examine a baseline scenario, a scenario involving increased ransomware activity, and a scenario involving higher-than-expected recovery costs. The purpose is not to predict the future with certainty, but to understand how sensitive the investment decision is to plausible changes in the underlying parameters.

Where the probability distributions of key variables cannot be estimated reliably, sensitivity analysis and robust optimization may be more appropriate than assigning precise probabilities without sufficient evidence. Existing research has demonstrated the value of stochastic and robust approaches for cybersecurity investment decisions under uncertain risk estimates (Zhang et al., 2018; Schmidt et al., 2021).

V. DISCUSSION

5.1. Implications for Cybersecurity Investment Theory

The proposed model contributes to the cybersecurity investment literature by integrating threat probability, potential loss, control effectiveness, implementation cost, and resource constraints into a common decision framework. Traditional risk assessments often rank threats by severity or likelihood, while investment decisions may be made separately through budget negotiations, compliance reviews, or technical recommendations. The proposed approach provides a structured means of connecting these activities.

The model also reflects the economic perspective that cybersecurity spending should be evaluated in relation to the losses it is expected to prevent or reduce. Gordon and Loeb (2002) established a foundational economic model for information-security investment, while subsequent research has examined the selection and allocation of controls under varying organizational and threat conditions. More recent work has explored optimization approaches that account for uncertainty, multiple risk objectives, and the interaction between security investment and organizational decision-making (Fedele & Roner, 2022; Schmidt et al., 2021).

The contribution of the present framework is not the claim that a single mathematical formulation can capture every cybersecurity investment decision. Rather, it offers a transparent baseline model that can be extended to accommodate organizational priorities, uncertainty, implementation dependencies, and mandatory controls.

5.2. Implications for Cybersecurity Managers

For cybersecurity managers, the model offers a way to connect technical assessments with financial planning. Security teams can estimate the expected losses associated with priority threats, identify controls capable of reducing those losses, and present management with alternative investment portfolios.

This approach may be particularly useful when cybersecurity competes with other operational priorities for limited funding. Instead of requesting a budget based exclusively on a list of recommended technologies, security leaders can explain which risks each proposed control addresses, the estimated reduction in expected loss, and the consequences of not implementing it.

The model can also support phased implementation. When the current budget cannot cover every desirable control, the organization can identify a feasible first-stage portfolio and reassess its priorities during subsequent budgeting cycles. This should not mean postponing essential safeguards indefinitely. Controls required by law, regulation, contractual obligations, or a formally approved risk-treatment plan should be treated as mandatory constraints rather than optional investments competing only on economic efficiency.

The model's recommendations should be reviewed by technical specialists and business stakeholders before implementation. The output is a decision aid, not an automatic substitute for professional judgment. Management remains responsible for deciding whether the estimated residual risk is acceptable and whether the assumptions reflect the organization's operating environment.

5.3. Implications for Small and Medium-Sized Enterprises

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Small and medium-sized enterprises (SMEs) may benefit from structured investment prioritization because they often face competing demands for limited financial, technical, and human resources. However, they may also lack the incident records, specialist personnel, and detailed cost data required to populate a sophisticated quantitative model.

The framework can be adapted to these conditions by beginning with a manageable number of material threat scenarios and a short list of realistic controls. Probability and impact estimates may initially be expressed using documented ordinal categories, provided that any conversion to numerical values is transparent and consistently applied. Where monetary loss estimates are available, they can be used directly; where they are not, managers should avoid presenting qualitative ratings as precise financial estimates.

External guidance, including NIST risk-assessment guidance and the ISO/IEC 27005 risk-management standard, can help organizations establish a repeatable process for identifying threats, assessing consequences, and documenting treatment decisions (NIST, 2012; ISO, 2022b). The resulting model should remain proportionate to the organization's size, risk exposure, and decision-making capacity.

For SMEs, the primary benefit may be improved discipline in prioritization rather than mathematical complexity. A simple, documented model that is reviewed regularly may provide greater practical value than a sophisticated model populated with unreliable estimates.

5.4. Implications for Governance and Accountability

A quantitative recommendation is only as reliable as the assumptions and evidence supporting it. Organizations should therefore establish governance procedures for the information used in the model. These procedures should identify who is responsible for estimating threat probabilities, assigning loss values, validating control effectiveness, approving cost assumptions, and reviewing the resulting portfolio.

Each recommendation should be traceable to its underlying data and assumptions. This enables decision-makers to explain why a control was selected, why another was deferred, and what residual risk remains. It also makes it easier to update the model when business processes change, new vulnerabilities emerge, or the effectiveness of existing controls is reassessed.

Risk acceptance should be documented separately from the model's mathematical output. A low residual expected loss does not necessarily mean that a risk is acceptable, particularly where a scenario could cause severe operational disruption, harm individuals, violate legal obligations, or threaten organizational survival. Governance should therefore combine quantitative optimization with risk appetite, regulatory requirements, and informed managerial judgment.

5.5. Implications for Compliance and Security Standards

The framework can support risk-based implementation of recognized cybersecurity standards and frameworks, including the NIST Cybersecurity Framework and ISO/IEC 27001. These frameworks provide organizational structures for identifying, managing, and monitoring cybersecurity risks, while the proposed optimization model offers a quantitative method for comparing possible control portfolios within resource constraints (NIST, 2018; ISO, 2022a).

The relationship should be understood as complementary. A mathematical model does not establish compliance on its own, and a portfolio that minimizes expected loss may not satisfy all applicable legal, regulatory, contractual, or certification requirements. Mandatory controls must be represented explicitly, and the organization must separately verify that implementation and operating practices meet the relevant requirements.

The model can nevertheless help prioritize discretionary investments once mandatory obligations have been identified. It can also help management explain the financial and risk implications of additional controls, subject to the limitations of the available evidence.

VI. LIMITATIONS OF THE PROPOSED MODEL

Several limitations should be considered when interpreting the framework.

First, the quality of the output depends on the reliability of the input estimates. Cyberattack probabilities and financial impacts are difficult to estimate, especially where incidents are underreported or the organization has limited historical data. Poor estimates can produce a mathematically optimal portfolio that is unsuitable for the actual environment.

Second, the baseline model represents control effectiveness as a proportional reduction in expected loss. This simplification may not adequately capture controls that operate at different stages of an attack, depend on one another, or produce threshold effects. For example, a detection control may have limited value without an effective response process. Future implementations should incorporate dependencies, overlapping coverage, and diminishing or increasing returns where evidence supports doing so.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Third, the model focuses on expected loss. This measure can obscure low-probability events with catastrophic consequences. Two portfolios may have similar expected losses while differing substantially in their exposure to extreme outcomes. Organizations facing such risks should supplement the model with risk thresholds, worst-case scenarios, tail-risk measures, or multi-objective optimization.

Fourth, the basic formulation assumes binary control selection. In practice, controls may be implemented at different maturity levels, scaled across business units, or deployed incrementally. A binary formulation may therefore oversimplify implementation decisions. Mixed-integer or continuous-variable extensions could represent investment levels, implementation phases, or varying levels of control coverage.

Fifth, implementation costs may not capture the full lifecycle burden of a control. Licensing, integration, training, maintenance, monitoring, staffing, and operational disruption can materially affect its true cost. A practical implementation should use a defined cost horizon and account for recurring expenditure as well as initial deployment costs.

Sixth, the model does not explicitly represent strategic attackers who change their behaviour in response to an organization's defenses. Nor does it fully capture the wider effects of shared suppliers, interconnected systems, or security investments by other organizations. Such relationships may alter both the probability and impact of incidents.

Finally, the numerical example in Section 4 is illustrative. It demonstrates the model's mechanics but does not constitute empirical validation. The framework's performance and practical usefulness must be tested with realistic data and compared with existing decision-making approaches before strong claims can be made about its superiority.

VII. DIRECTIONS FOR FUTURE RESEARCH

Future research should prioritize empirical validation of the proposed model across organizations with different sizes, sectors, and cybersecurity maturity levels. Case studies could examine whether model-generated portfolios differ from those selected through conventional risk-ranking or expert-judgment processes, and whether these differences lead to measurable improvements in risk reduction or resource utilization.

A second direction is to improve the treatment of uncertainty. Researchers could estimate probability distributions for threat occurrence, financial impact, and control effectiveness using incident records, vulnerability data, security assessments, and expert elicitation. Where reliable distributions are unavailable, robust optimization and structured sensitivity analysis could help determine whether recommendations remain useful under a range of plausible conditions.

Third, future work could investigate multi-objective models that balance expected residual loss with implementation cost, regulatory compliance, resilience, and the number of high-priority threats brought below defined risk thresholds. Such models would better reflect the fact that organizations may value broad risk coverage as well as reductions in total expected loss. Existing research on bi-objective cybersecurity optimization provides a foundation for this direction (Schmidt et al., 2021).

Fourth, control dependencies and overlapping effectiveness deserve further attention. A more advanced formulation could distinguish preventive, detective, responsive, and recovery controls and represent how their combined effectiveness depends on deployment quality and operational integration. This would help reduce the risk of overestimating the benefits of controls that address the same weakness or rely on the same underlying infrastructure.

Fifth, researchers could develop user-friendly decision-support tools for SMEs. Such tools could provide guided data entry, transparent assumptions, scenario comparison, and explanations of the reasons behind each recommendation. The aim should be to make quantitative decision support accessible without concealing uncertainty or presenting model outputs as objectively certain answers.

Finally, longitudinal studies could assess whether the adoption of risk-based investment models improves decision transparency, budget allocation, control implementation, and incident outcomes over time. These studies would help distinguish the immediate value of better planning from the longer-term effects of cybersecurity investment on organizational resilience.

VIII. CONCLUSION

Cybersecurity investment under resource constraints requires organizations to make difficult choices about which security controls to implement, which risks to address first, and which exposures must temporarily remain untreated. Decisions based solely on threat severity, technology cost, compliance pressure, or professional intuition may overlook important differences in threat probability, potential loss, control effectiveness, and resource requirements.

This paper has proposed a quantitative decision-support framework for selecting security controls according to their estimated contribution to reducing expected residual loss, subject to financial and operational constraints.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

By representing threat scenarios, baseline risk, control effectiveness, implementation costs, and mandatory requirements within a common optimization model, the framework offers a transparent basis for comparing feasible investment portfolios.

The illustrative analysis demonstrates how a constrained budget can be allocated by considering the combined effects of controls across multiple threat scenarios. It also shows that the preferred portfolio depends on the assumptions and risk profile of the organization, rather than on any universal ranking of security technologies. The results are illustrative and should not be interpreted as empirical evidence that a particular portfolio is generally superior.

The practical value of the framework ultimately depends on the quality of its inputs, the realism of its assumptions, and its integration with organizational governance. It should be used alongside recognized risk-management practices, technical expertise, compliance obligations, and explicit decisions about risk acceptance. Further empirical testing, uncertainty modelling, and incorporation of control dependencies are necessary to establish its effectiveness in real-world settings.

Within these boundaries, risk-based optimization can help organizations move from fragmented security spending toward more consistent, evidence-informed investment decisions. The objective is not to eliminate cybersecurity risk at any cost, but to use limited resources in a way that reduces the most consequential exposures while maintaining accountability for the risks that remain.

REFERENCES

1) Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613. https://doi.org/10.1126/science.1130992
2) Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 51*(2), 78–83.
3) Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002
4) Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS)*.
5) Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87–92. https://doi.org/10.1145/1005817.1005828
6) Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet, 15*(10), Article 324. https://doi.org/10.3390/fi15100324
7) Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys, 36*(1), 157–187. https://doi.org/10.1111/joes.12456
8) Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274
9) Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity, 6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005
10) Herath, H. S. B., & Herath, T. (2008). Investments in information security: A real options perspective with Bayesian Poisson learning. *Journal of Management Information Systems, 25*(3), 337–375.
11) International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC Standard No. 27001:2022).* ISO.
12) International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection—Guidance on managing information security risks (ISO/IEC Standard No. 27005:2022).* ISO.
13) Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare industry. *MIS Quarterly, 38*(2), 451–471.
14) National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1
15) National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.6

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

16) Paul, J. A., & Zhang, M. (2021). Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. *European Journal of Operational Research, 291*(1), 349–364.
17) Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135.
18) Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences, 13*(1), Article 395. https://doi.org/10.3390/app13010395
19) Sawik, T. (2022). A linear model for optimal cybersecurity investment in Industry 4.0 supply chains. *International Journal of Production Research, 60*(4), 1368–1385. https://doi.org/10.1080/00207543.2020.1856442
20) Schmidt, A., Albert, L. A., & Zheng, K. (2021). Risk management for cyber-infrastructure protection: A bi-objective integer programming approach. *Reliability Engineering & System Safety, 207*, Article 107093. https://doi.org/10.1016/j.ress.2020.107093
21) Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. *IEEE Access, 11*, 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670
22) Zhang, H., Chari, K., & Agrawal, M. (2018). Decision support for the optimal allocation of security controls. *Decision Support Systems, 115*, 92–104. https://doi.org/10.1016/j.dss.2018.10.001

 © Author(s) | CC BY 4.0 International License.